

## Ruckus SmartZone Configuration - Customer Guide

# ADENTRO

### Adentro Overview

Adentro provides consumers with an amazing WiFi experience at their favorite spots, while helping to grow local businesses by better engaging and targeting their customers. By offering a branded captive portal for your guest WiFi network, customers are given the ability to opt-in to targeted messaging sent using the Adentro platform.

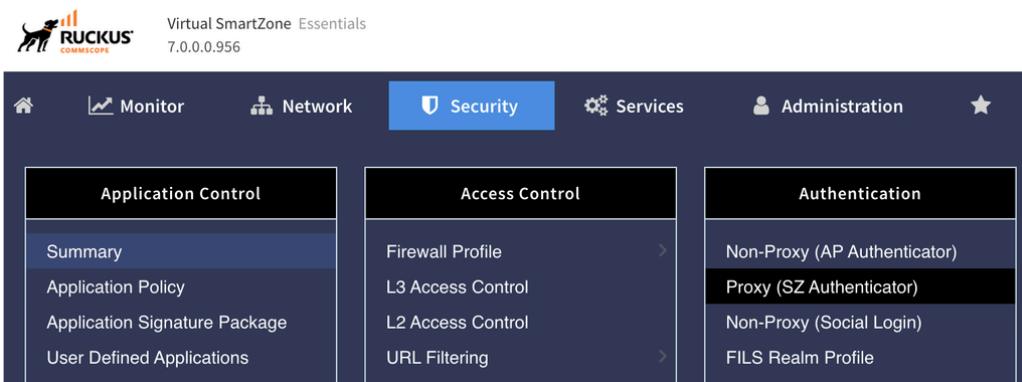
### Adentro Configuration

In order to associate your Ruckus access point(s) with your business information, Adentro will need the MAC address of each individual access point that will be broadcasting the integrated SSID. **Please forward your AP MAC address(es) to your Adentro Account Manager.** Without completion of this step, guests will receive a "404" error on the captive portal. **\*\* Disable any other guest networks that are running on other wireless networks to achieve the best results with Adentro \*\***

### Configure AAA

#### Authentication

1. Under Services and Profiles, select Authentication
2. Select the "Proxy (SZ Authenticator)" tab



The screenshot shows the Ruckus Virtual SmartZone Essentials interface. The top navigation bar includes icons for Home, Monitor, Network, Security (which is highlighted in blue), Services, Administration, and a star icon. Below the navigation is a main menu with three columns: Application Control, Access Control, and Authentication. The Authentication column is currently active, displaying five options: Non-Proxy (AP Authenticator), Proxy (SZ Authenticator) (which is highlighted in dark blue), Non-Proxy (Social Login), and FILS Realm Profile.

3. Select "Create"
4. Enter the following information:

**Name:** Adentro  
**Friendly Name:** Adentro  
**Description:** Adentro  
**Service Protocol:** RADIUS

#### Primary Server

**IP Address:** 54.69.8.147  
**Port:** 1812

**Secret:** 8fc40973252c42e196489d4a16849ff8

#### Secondary Server

**Enable Secondary Server:** checked

**IP Address:** 54.68.29.80

**Port:** 1812

**Secret:** 8fc40973252c42e196489d4a16849ff8

**Health Check Policy:** use default settings

#### Rate Limiting

**Maximum Outstanding Requests:** 0

**Threshold:** 0

**Sanity Time:** 10s

DETAILS	Protocol	RADIUS
Name	Adentro	
Manage By	System	
Description	Adentro	
IP Address/FQDN	54.69.8.147	
Port	1812	
Secondary IP Address/FQDN	54.68.29.80	
Port	1812	

#### Accounting

1. Under Services and Profiles, select "Accounting"
2. Select the "Proxy" tab
3. Select "Create"
4. Enter the following information:

**Name:** Adentro

**Description:** Accounting

**Service Protocol:** RADIUS Accounting

**Encryption:** TLS Unchecked

**Backup RADIUS:** Checked

#### **Primary Server:**

**IP Address:** 54.69.8.147

**Port:** 1813

**Secret:** 8fc40973252c42e196489d4a16849ff8

#### **Secondary Server:**

Enable Secondary Server

**IP Address:** 54.68.29.80

**Port:** 1813

**Secret:** 8fc40973252c42e196489d4a16849ff8

**Health Check Policy:** use default settings

#### Rate Limiting

**Maximum Outstanding Requests:** 0

**Threshold:** 0

**Sanity Time:** 10s



Name	AdentroAcct
Manage By	System
protocol	RADIUS
Description	Adentro
IP Address/FQDN	54.69.8.147
Port	1813
Enable Secondary Server	Yes
Secondary IP Address/FQDN	54.68.29.80
Port	1813
TLS Enabled	No

## Configure Hotspot Portal

1. Under Services and Profiles, find the "Hotspots & Portals" section
2. Select the "Hotspot (WISPr)" tab



Virtual SmartZone Essentials  
7.0.0.956

Home Monitor Network Security Services

**Hotspots & Portals**

- Guest Access
- Hotspot (WISPr) **
- Hotspot 2.0
- Web Auth
- UA Blacklist
- Portal Detection & Suppression
- WeChat
- Network Segmentation >

**Tunnels & Ports**

- Ruckus GRE
- SoftGRE
- IPsec
- Ethernet Port
- DiffServ
- CALEA
- Tunnel Encryption(DP)
- Multicast Forwarding

3. Select "Create"
4. Enter the following information:

**Portal Name:** Adentro

### Redirection

**Smart Client Support:** None

**Logon URL:** External

**Redirect URL:** <https://gateway.wifast.com/ruckus/smartzone/>

**Redirected MAC Format:** aa:bb:cc:dd:ee:ff

**Start Page:** "redirect to the following URL:" <https://gateway.wifast.com/online/>

**HTTPS Redirect:** checked

**Redirection**

Smart Client Support:  None  Enable  Only Smart Client Allowed

Logon URL:  Internal  External

Redirect unauthenticated user:

- \* Primary:
- Secondary:

\* Redirected MAC Format:

Start Page: After user is authenticated,

- Redirect to the URL that user intends to visit.  Redirect to the following URL:
- \*

HTTPS Redirect:  ON  OFF The AP will try to redirect HTTPS requests to the hotspot portal

### Walled Garden

gateway.wifast.com

#### Walled Garden / Traffic Class Profile

<input checked="" type="radio"/> Walled Garden	* Walled Garden Entry	<input type="button" value="Add"/>	<input type="button" value="Import CSV"/>	<input type="button" value="Cancel"/>	<input type="button" value="Delete"/>
Walled Garden Entry ▲					
<a href="#">gateway.wifast.com</a>					
1 records << 1 >>					

### Configure WLAN ↗

- Under "Wireless LANs", create a new WLAN or edit an existing one
- Enter the following information:

#### Authentication Options

**Authentication Type:** Hotspot (WISPr)

**Method:** Open

#### Encryption Options

**Method:** None

#### Hotspot Portal

**Hotspot (WISPr) Portal:** Adentro

**Bypass CNA:** unchecked

**Authentication Server:** check "Use the controller as proxy" and select "Adentro"

**Accounting Server:** check "Use the controller as proxy", select "Adentro", and send updates every 1 minute

#### Authentication Options

Authentication Type:  Standard usage (For most regular wireless networks)  Hotspot (WISPr)  Guest Access  Web Authentication  
 Hotspot 2.0 Access  Hotspot 2.0 Onboarding  WeChat

Method:  Open  802.1X EAP  MAC Address  802.1X EAP & MAC

#### Encryption Options

Method:  WPA2  WPA3  WPA2/WPA3-Mixed  OWE  OWE-Transition  WPA-Mixed  None

Encryption methods other than WPA3 and OWE will not be supported on 6GHz radio. Only WPA3 is used on 6GHz radio with WPA2/WPA3-Mixed mode.

#### Data Plane Options

#### Hotspot Portal

Hotspot (WISPr) Portal:

Bypass CNA:  OFF

Authentication Server:  ON  Use the Controller as Proxy  
    
 OFF Backup Authentication Service

Accounting Server:  ON  Use the Controller as Proxy  
   Send interim update every  Minutes (0-1440)

#### Wireless Client Isolation

We suggest isolating guest traffic to protect your network and other guests.

**Client Isolation:** On

**Isolate unicast & multicast packets:** On (for both)

#### RADIUS Options

**NAS ID:** AP MAC

**Delimiter:** Colon

**Called Station ID:** AP MAC

The screenshot shows two configuration pages for a wireless access point. The top section, "Wireless Client Isolation", includes settings for "Acct Delay Time" (OFF), "Client Isolation" (ON, isolating client traffic from all hosts on the same VLAN/subnet, ON, isolating unicast packets, ON, isolating multicast/broadcast packets, OFF, automatic support for VRRP/HSRP), and an "Isolation Whitelist" dropdown set to "Gateway Only (Automatic)" with a note about whitelisting requirements. The bottom section, "RADIUS Options", includes fields for "NAS ID" (WLAN BSSID selected), "Delimiter" (Colon selected), "NAS Request Timeout" (3 seconds), "NAS Max Number of Retries" (2 times), "NAS Reconnect Primary" (5 minutes), "Called Station ID" (AP MAC selected), "NAS IP" (Disabled selected), and "Single Session ID Accounting" (OFF). A note states that APs will maintain one accounting session for client roaming.

## Configure Northbound Interface

The northbound interface must be configured so that Adentro servers can make requests to decrypt MAC addresses they receive on portal requests. Without this, Adentro cannot determine which location the AP belongs to or which customer the client device belongs to.

- Under "Administration", select "WISPr Northbound Interface"
- Check "Enable Northbound Portal Interface Support"
- Enter username "ruckus" (lowercase "r"), and a secure password.

The screenshot shows the "WISPr Northbound Interface" tab selected in the navigation bar. Below it, a note says to set the northbound portal interface password for 3rd party applications. The "Enable Northbound Portal Interface Support" switch is ON. Input fields for "User Name" (ruckus) and "Password" (redacted) are shown. At the bottom are "Refresh", "OK", and "Cancel" buttons.

You will need to ensure the northbound interface is reachable over the internet on a static IP, so that Adentro servers can reach it. It should be available on TCP port 9443. Ensure any firewalls and port forwarding will allow this (See Firewall Rules section below).

To test that the northbound interface is available, you can use the following curl command to see if you get an expected response. Be sure to replace the IP and password in the command.

```

1 $ curl -X POST https://[YOUR NORTHBOUND INTERFACE IP HERE]:9443/portalintf -H 'Content-Type: application/json'
-k -d '{
2     "Vendor": "ruckus",
3     "APIVersion": "1.0",

```

```

4     "RequestPassword": "YOUR PASSWORD HERE",
5     "RequestCategory": "GetConfig",
6     "RequestType": "Decrypt",
7     "Data": "123456781234",
8 }'

```

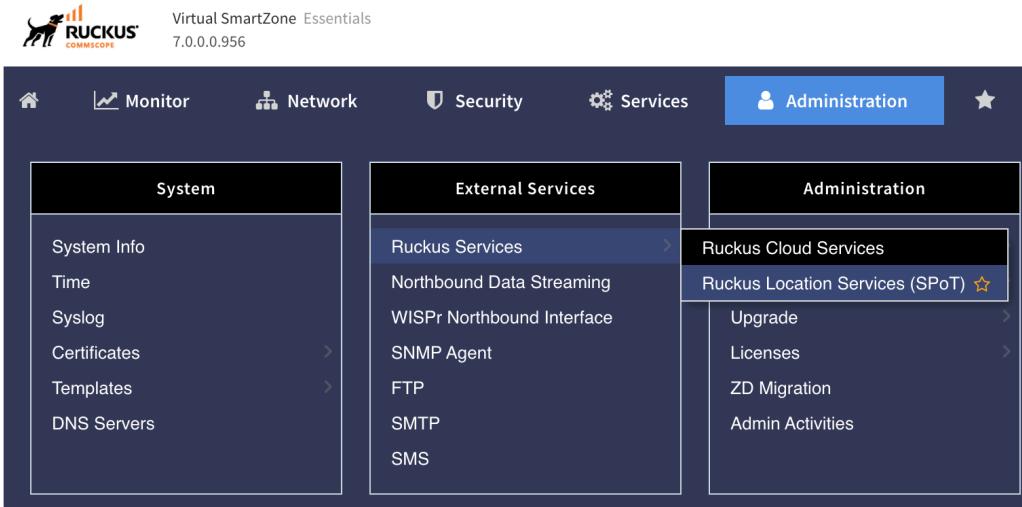
You should see a response like the following:

```
1 {"ResponseCode":200,"APIVersion":"1.0","Data":"123456781234","Vendor":"Ruckus","ReplyMessage":"OK"}
```

After confirming it works, please share the northbound interface IP and password with your Adentro account manager.

## Configure Location Services

1. Select "Administration" > "External Services" > "Ruckus Services" > select "Ruckus Location Services (SPoT)"



2. Choose "Create"

3. Enter the following information:

**Venue Name:** [Touch base with your Adentro Account Manager to get receive this unique value]

**Server FQDN or IP Address:** mqtt.service.zp.cntr.io

**Port:** 8883

**Password:** [Touch base with your Adentro Account Manager to get receive this unique value]

**TLS Version:** tlsv1.2

4. From the main menu, choose "Network" > "Wireless LANs"

5. Edit your guest zone

6. Scroll down to "Advanced Options"

7. Enable "Location Based Service" and select the name of the venue you created in the previous step

Load Balancing:  Based on Client Count  [?] Based on Capacity  Disabled

Make sure background scan is enabled on radios you would like to run load balancing.

OFF Limit 2.4Ghz Clients to 25 %

[?] Steering Mode:  Basic  Proactive  Strict

[?] Sticky Client Steering:  OFF SNR Threshold 15 dB NBRAP % Threshold 20 %

[?] Location Based Service:  ON  hhR7RV15Xvly:

Hotspot 2.0 Venue Profile:  OFF No data available

[?] Client Admission Control:

<b>2.4 GHz Radio</b> <input type="radio"/> OFF Min Client Count 10 Max Radio Load 75 % Min Client Throughput 0 Mbps	<b>5 GHz Radio</b> <input type="radio"/> OFF Min Client Count 20 Max Radio Load 75 % Min Client Throughput 0 Mbps
---	---

You will need to allow traffic on TCP port 8883 for location services to work. Please ensure any firewalls you have are updated to allow this traffic.

## Firewall Rules

### AAA / RADIUS

TCP/1812, UDP/1813 - Source: SmartZone Controller IP - Destination: RADIUS servers (54.69.8.147 & 54.68.29.80)

### WISPr / Guest WiFi

TCP/8099 - Source: Guest Devices (Clients) - Destination: SZ Controller

TCP/9443 - Source: gateway.wifast.com (54.68.113.153, 54.68.53.46, 54.68.126.162) - Destination: SZ Controller

### Location Services (MQTT)

TCP/8883 - Source: SmartZone Controller IP - Destination: mqtt.service.zp.cntr.io (34.210.1.57, 44.238.194.89, 44.234.214.75)